MONITORING OF FAILURE TOLERANCE FOR AN AUTOMATION INSTALLATION

[0001] The invention relates to a method for monitoring a failure tolerance for an automation installation. The automation installation is used to operate or perform a process, for example generating electric power from nuclear power, by means of a controlled system. The automation installation is meant to be failure safe and, to this end, has at least two control apparatuses that alternately control the controlled system. In the event of failure of the currently controlling control apparatus, the arrangement changes over to another control apparatus. In this context, there must be the assurance that the process can continue to be operated safely during changeover.

[0002] The described high-availability solution of installation control by means of at least two control apparatuses reduces any standstill periods that arise for the automation installation to a minimum. The development of high-availability solutions of this kind is currently very cost intensive, however. The primary accomplishment of such an automation system is automatic failover, that is to say changeover, in the event of failure of one of the control apparatuses, for example as a result of CPU failure (CPU—central processing unit). Control of the process can then be continued on a backup CPU. This failover is never totally without repercussions for the process. Usually, what is demanded is smooth failover, that is to say that the output of the control apparatuses, that is to say the inputs of the controlled system of the process, must have no discernible jumps that are caused not by an alteration in the controlled system but rather exclusively on account of failure of the control apparatus. The outputs must thus behave constantly, so that the control signal for the controlled system, that is to say the sequence of control outputs, must not fluctuate beyond a predetermined measure due to failure.

[0003] Usually, a limited period of time is tolerated in which the control outputs transmitted to the controlled system retain their last value before control of the controlled system is then continued by the backup CPU. Influencing factors for the down time that is to be expected, during which the constant control output is output, are the failover response of the control apparatuses and the failover response of the controlled system. Depending on the peripheral components used that are actuated by the control apparatuses and monitor and control the process, one of the two influencing factors is normally dominant.

[0004] Today, the user of an automation installation himself has to judge whether the process to be controlled can tolerate the effects of a failover. A failover must not result in destabilization of the process. Nowadays, the user answers these questions on the basis of empirical values about his process or empirical values about similar processes.

[0005] The invention is based on the object of checking the failover response of an automation installation to determine whether the automation installation has sufficient failure tolerance toward failure of one of its control apparatuses.

[0006] The invention achieves the object by means of the subjects of the independent patent claims. Advantageous developments of the invention are obtained by means of the features of the dependent patent claims.

[0007] The method according to the invention sets out from the automation installation described at the outset, in which a controlled system is used to perform a process, that is to say, by way of example, that electric power is generated from nuclear power, bottles are filled, crude oil is refined or a building is heated. The automation installation has at least two control apparatuses provided that alternately control the controlled system during normal operation, which comprises output of control outputs. In this context, alternately means that failure of the currently controlling control apparatus prompts changeover to another of the control apparatuses. During changeover, the controlled system continues to be operated in controller-less fashion, the changeover requiring a period of time that is referred to in this case as a down time. The control apparatuses may each be a programmable logic controller (PLC), for example.

[0008] The automation installation is now monitored by the method to determine whether it is failure tolerant. In other words, a check is performed to determine whether failure of one control apparatus and changeover to another control apparatus is possible without this involving the process reaching a predetermined, undesirable critical state, that is to say the controlled system adopting an undesirable operating state, within the down time.

[0009] On the basis of the method according to the invention, this is accomplished by virtue of at least one operating point that is possible for the controlled system during normal operation being ascertained. In this context, an operating point describes a possible operating state of the controlled system and can be represented or described as a vector of operating variables, for example. Such an operating variable may be a temperature, a rotational speed or a conveying speed in each case, for example. These operating variables each describe a state of at least one peripheral component, that is to say of a sensor or an actuator, for example, of the automation installation. Overall, the operating point, i.e. the operating state of the whole controlled system, is then obtained from all of the operating variables.

[0010] For each operating point, a respective check is now performed to determine whether, on the basis of this operating point, it is possible to change over between the control apparatuses and, in this context, controller-less operation is possible safely for the down time. This is accomplished by simulating respective controller-less operation for each operating point for the duration of the down time and thereby ascertaining a state trajectory for the controlled system that starts out from the operating point. The state trajectory is thus compiled from a temporal sequence of operating points that are obtained from the changeover time onward during controller-less operation in accordance with the simulation. The respective state trajectory has a check performed for it to determine whether it fails to meet a predetermined safety criterion. If need be, a predetermined protective measure is initiated to avoid this operating state from which changeover has led to the critical state trajectory.

[0011] In connection with the invention, the term controlled system covers the at least one peripheral component that is provided for controlling the process in the automation installation, that is to say the sensors and actuators of the automation installation, the communication network that couples the control apparatuses to the at least one peripheral component, and the process itself, that is to say the installation components monitored and/or controlled by the peripheral components, such as conveyor belts, gantries or pipes, for example.

[0012] The invention has the advantage that a method is now provided that assists in estimating the effects of a changeover action on the process and thus reduces the risk